Exhibit A

Data Use, Security, and Confidentiality Requirements

1. Definitions

In addition to the definitions set out in section 2, Definitions, of the Contract, the definitions below apply to this Exhibit:

“**Authorized User**” means an individual or individuals with an authorized business need to access HCA’s Confidential Information under this Contract.

“**Client**” means an individual who is eligible for or receiving Medicaid services.

“**Data**” means the information that is disclosed or exchanged as described by this Contract. For purposes of this Contract, Data means the same as “Confidential Information.”

“**Disclosure**” means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

“**Personal Information**” means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use, or receipt of governmental services or other activities, address, telephone numbers, social security numbers, driver’s license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

“**ProviderOne**” means the Medicaid Management Information System (MMIS), which is the State’s Medicaid payment system managed by HCA.

“**Regulation**” means any federal, state, or local regulation, rule, or ordinance.

“**Use**” includes the sharing, employment, application, utilization, examination, or analysis of Data.

1. Description of Data
   1. Enrollment and Participant account information. The Data will be provided on an ad hoc, weekly, monthly and annual basis (depending on account type and administrative purpose) during the term of the Contract via a secure file transfer protocol (SFTP).
   2. Data Use Purpose. The purpose for sharing the Data is for the Contractor to correctly enroll Participants and administer the portfolio of tax-advantaged accounts.
   3. The Data to be shared is:
2. Participant Last name
3. Participant First name
4. Participant Social Security Number
5. Participant’s Agency of Record
6. Claim Amount
7. Account Type (FSA, DCAP, HBA and HSA)
   1. The Data may be linked with the following system:
      1. Pay1
8. Data Classification

The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the state of Washington Chief Information Officer. (See Section 4, Data Security, of Securing IT Assets Standards No. 141.10 in the State Technology Manual at <https://ocio.wa.gov/policy/securing-information-technology-assets>. Section 4 is hereby incorporated by reference.)

The Data that is the subject of this Contract may be in any of the Categories indicated below:

Category 1 – Public Information

Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

Category 2 – Sensitive Information

Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3 – Confidential Information

Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

* Personal Information about individuals, regardless of how that information is obtained;
* Information concerning employee personnel records;
* Information regarding IT infrastructure and security of computer and telecommunications systems;

Category 4 – Confidential Information Requiring Special Handling.

Category 4 Data is information that is specifically protected from disclosure and for which:

* Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements;
* Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

1. Constraints on Use of Data
   1. The Data being shared/accessed is owned and belongs to HCA.
   2. This Contract does not constitute a release of the Data for the Contractor’s discretionary use. Contractor must use the Data received or accessed under this Contract only to carry out the purpose of this Contract. Any analyses, use, or reporting that is not within the Purpose of this Contract is not permitted without HCA’s prior written consent.
   3. Any disclosure of Data contrary to this Contract is unauthorized and is subject to penalties identified in law.
2. Security of Data
   1. Data Protection

The Contractor must protect and maintain all Confidential Information gained by reason of this Contract, information that is defined as confidential under state or federal law or regulation, or Data that HCA has identified as confidential, against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor to employ reasonable security measures, which include restricting access to the Confidential Information by:

* + 1. Allowing access only to staff that have an authorized business requirement to view the Confidential Information; and
    2. Physically securing any computer, documents, or other media containing the Confidential Information.
  1. Data Security Standards

Contractor must comply with the Data Security Requirements set out in Attachment 1, *Confidential Information Security Requirements*, and the Washington OCIO Security Standard, 141.10, which will include any successor, amended, or replacement regulation (<https://ocio.wa.gov/policy/securing-information-technology-assets>.) The Security Standard 141.10 is hereby incorporated by reference into this Contract.

* 1. Data Disposition

For the purposes of this section “fiscal year” is from July 1 to June 30.

Upon request by HCA, at the end of the Contract term, when no longer needed, or 6 years after the end of the fiscal year in which the Data is received, Confidential Information/Data must be returned to HCA or disposed of as set out in Attachment 1, *Confidential Information Security Requirements*,except as required to be maintained for compliance or accounting purposes.

1. Data Confidentiality and Non-Disclosure
   1. Data Confidentiality

The Contractor will not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with the purpose of this Contract, except:

* as provided by law; or
* with the prior written consent of the person or personal representative of the person who is the subject of the Confidential Information.
  1. Non-Disclosure of Data

The Contractor must ensure that all employees or Subcontractors who will have access to the Data described in this Contract (including both employees who will use the Data and IT support staff) are instructed and made aware of the use restrictions and protection requirements of this Contract before gaining access to the Data identified herein. The Contractor will also instruct and make any new employee aware of the use restrictions and protection requirements of this Contract before they gain access to the Data.

The Contractor will ensure that each employee or Subcontractor who will access the Data signs the *User Agreement on Non-Disclosure of Confidential Information*, Exhibit B hereto. The Contractor will retain the signed copy of the *User Agreement on Non-Disclosure of Confidential Information* in each employee’s personnel file for a minimum of six years from the date the employee’s access to the Data ends. The documentation must be available to HCA upon request.

* 1. Penalties for Unauthorized Disclosure of Data

State laws (including RCW 74.04.060 and RCW 70.02.020) and federal regulations (including HIPAA Privacy and Security Rules, 45 CFR Part 160 and Part 164; Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR, Part 2; and Safeguarding Information on Applicants and Beneficiaries, 42 CFR Part 431, Subpart F) prohibit unauthorized access, use, or disclosure of Confidential Information. The Contractor must comply with all applicable federal laws and regulations concerning collection, use, and disclosure of Personal Information and PHI. Violation of these laws may result in criminal or civil penalties or fines.

The Contractor accepts full responsibility and liability for any noncompliance by itself, its employees, and its Subcontractors with these laws and any violations of the Contract.

1. Data Shared with Subcontractors

If Data access is to be provided to a Subcontractor under this Contract, the Contractor must include all of the Data security terms, conditions and requirements set forth in this Contract in any such Subcontract. However, no subcontract will terminate the Contractor's legal responsibility to HCA for any work performed under this Contract nor for oversight of any functions and/or responsibilities it delegates to any subcontractor

1. Data Breach Notification
   1. The Breach or potential compromise of Data must be reported to the HCA Privacy Officer at [PrivacyOfficer@hca.wa.gov](mailto:PrivacyOfficer@hca.wa.gov) within 2 business days of discovery. If the Contractor does not have full details, it will report what information it has, and provide full details within 15 business days of discovery. To the extent possible, these reports must include the following:
      1. The identification of each individual whose PHI has been or may have been improperly accessed, acquired, used, or disclosed;
      2. The nature of the unauthorized use or disclosure, including a brief description of what happened, the date of the event(s), and the date of discovery;
      3. A description of the types of PHI involved;
      4. The investigative and remedial actions the Contractor or its Subcontractor took or will take to prevent and mitigate harmful effects, and protect against recurrence;
      5. Any details necessary for a determination of the potential harm to individuals whose PHI is believed to have been used or disclosed and the steps those individuals should take to protect themselves; and
      6. Any other information HCA reasonably requests.
   2. The Contractor must take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or HCA including but not limited to 45 C.F.R. Part 164, Subpart D; RCW 42.56.590; RCW 19.255.010; or WAC 284-04-625.
   3. If notification of the Breach or possible Breach must, in the judgement of HCA, be made under the HIPAA Breach Notification Rule, or RCW 42.56.590 or RCW 19.255.010, or other law or rule, then:
      1. HCA may choose to make any required notifications to the individuals, to the U.S. Department of Health and Human Services (DHHS) Secretary, and to the media, or direct Contractor to make them or any of them.
      2. In any case, Contractor will pay the reasonable costs of notification to individuals, media, and governmental agencies and of other actions HCA reasonably considers appropriate to protect HCA clients, such as paying for regular credit watches in some cases.
      3. Contractor will compensate HCA clients for harms caused to them by any Breach or possible Breach.
   4. Any breach of this clause may result in termination of the Contractor and the demand for return or disposition, as described in Section 5.3, of all Confidential Information.
   5. Contractor’s obligations regarding Breach notification survive the termination of this Contract and continue for as long as Contractor maintains the Confidential Information and for any Breach or possible Breach at any time.
2. HIPAA Compliance
   1. This section of the DSA is the Business Associate Agreement required by HIPAA. The Contractor is a “Business Associate” of HCA as defined in the HIPAA Rules.
   2. HIPAA Point of Contact. The point of contact for the Contractor for all required HIPAA-related reporting and notification communications from this section*:*

HCA Privacy Officer

Washington State Health Care Authority

626 8th Avenue SE

PO Box 42700

Olympia, WA 98504-2700

Telephone: 360-725-1116

E-mail: [PrivacyOfficer@hca.wa.gov](mailto:PrivacyOfficer@hca.wa.gov)

* 1. Compliance. Business Associate must perform all DSA duties, activities and tasks in compliance with HIPAA, the HIPAA Rules, and all attendant regulations as promulgated by the U.S. Department of Health and Human Services, Office for Civil Rights, as applicable.
  2. Use and Disclosure of PHI. Business Associate is limited to the following permitted and required uses or disclosures of PHI:
     1. Duty to Protect PHI. Business Associate must protect PHI from, and will use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to ePHI, to prevent the unauthorized Use or disclosure of PHI for as long as the PHI is within its possession and control, even after the termination or expiration of this DSA.
     2. Minimum Necessary Standard. Business Associate will apply the HIPAA Minimum Necessary standard to any Use or disclosure of PHI necessary to achieve the purposes of this DSA. See 45 CFR 164.514 (d)(2) through (d)(5).
     3. Disclosure as Part of the Provision of Services. Business Associate will only Use or disclose PHI as necessary to perform the services specified in this DSA or as required by law, and will not Use or disclose such PHI in any manner that would violate Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information) if done by Covered Entity, except for the specific uses and disclosures set forth below.
     4. Use for Proper Management and Administration. Business Associate may Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
     5. Disclosure for Proper Management and Administration. Business Associate may disclose PHI for the proper management and administration of Business Associate, subject to HCA approval, or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.
     6. Impermissible Use or Disclosure of PHI. Business Associate must report to the contact identified in Subsection 9.2 in writing all Uses or disclosures of PHI not provided for by this DSA within five (5) business days of becoming aware of the unauthorized Use or disclosure of PHI, including Breaches of unsecured PHI as required at 45 CFR 164.410 (Notification by a Business Associate), as well as any Security Incident of which it becomes aware. Upon request by HCA, Business Associate will mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or disclosure.
     7. Failure to Cure. If HCA learns of a pattern or practice of the Business Associate that constitutes a violation of the Business Associate’s obligations under the terms of this DSA and reasonable steps by the Business Associate do not end the violation, HCA may terminate this DSA, if feasible. In addition, If Business Associate learns of a pattern or practice of its Subcontractors that constitutes a violation of the Business Associate’s obligations under the terms of their contract and reasonable steps by the Business Associate do not end the violation, Business Associate must terminate the Subcontract, if feasible.
     8. Termination for Cause. Business Associate authorizes immediate termination of this DSA by HCA, if they determine that Business Associate has violated a material term of this Business Associate Agreement. HCA may, at their sole option, offer Business Associate an opportunity to cure a violation of this Business Associate Agreement before exercising a termination for cause.
     9. Consent to Audit. Business Associate must give reasonable access to PHI, its internal practices, records, books, documents, electronic data and/or all other business information received from, or created or received by Business Associate on behalf of HCA, to the Secretary of DHHS and/or to HCA for use in determining compliance with HIPAA privacy requirements.
     10. Obligations of Business Associate Upon Expiration or Termination. Upon expiration or termination of this DSA for any reason, with respect to PHI received from HCA, or created, maintained, or received by Business Associate, or any Subcontractors, on behalf of HCA, Business Associate must:

1. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to HCA or destroy the remaining PHI that the Business Associate or any Subcontractors still maintain in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to Electronic Protected Health Information to prevent Use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate or any Subcontractors retain the PHI;
4. Not Use or disclose the PHI retained by Business Associate or any Subcontractors other than for the purposes for which such PHI was retained and subject to the same conditions set out in Subsection 9.4 *Use and Disclosure of PHI* that applied prior to termination; and
5. Return to HCA or destroy the PHI retained by Business Associate, or any Subcontractors, when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.
   1. Survival. The obligations of the Business Associate under this section will survive the termination or expiration of this DSA.
   2. Individual Rights.
      1. Accounting of Disclosures.
6. Business Associate will document all disclosures, except those disclosures that are exempt under 45 CFR 164.528, of PHI and information related to such disclosures.
7. Within ten (10) business days of a request from HCA, Business Associate will make available to HCA the information in Business Associate’s possession that is necessary for HCA to respond in a timely manner to a request for an accounting of disclosures of PHI by the Business Associate. See 45 CFR 164.504(e)(2)(ii)(G) and 164.528(b)(1).
8. At the request of HCA or in response to a request made directly to the Business Associate by an Individual, Business Associate will respond, in a timely manner and in accordance with HIPAA and the HIPAA Rules, to requests by Individuals for an accounting of disclosures of PHI.
9. Business Associate record keeping procedures will be sufficient to respond to a request for an accounting under this section for the six (6) years prior to the date on which the accounting was requested.
   * 1. Access
10. Business Associate will make available PHI that it holds that is part of a Designated Record Set when requested by HCA or the Individual as necessary to satisfy HCA’s obligations under 45 CFR 164.524 (Access of Individuals to Protected Health Information).
11. When the request is made by the Individual to the Business Associate or if HCA ask the Business Associate to respond to a request, the Business Associate must comply with requirements in 45 CFR 164.524 (Access of Individuals to Protected Health Information) on form, time and manner of access. When the request is made by HCA, the Business Associate will provide the records to HCA within ten (10) business days.
    * 1. Amendment.
12. If HCA amends, in whole or in part, a record or PHI contained in an Individual’s Designated Record Set and HCA has previously provided the PHI or record that is the subject of the amendment to Business Associate, then HCA will inform Business Associate of the amendment pursuant to 45 CFR 164.526(c)(3) (Amendment of Protected Health Information).
13. Business Associate will make any amendments to PHI in a Designated Record Set as directed by HCA or as necessary to satisfy HCA’s obligations under 45 CFR 164.526 (Amendment of Protected Health Information).
    1. Subcontracts and other Third Party Agreements. In accordance with 45 CFR 164.502(e)(1)(ii), 164.504(e)(1)(i), and 164.308(b)(2), Business Associate must ensure that any agents, Subcontractors, independent contractors or other third parties that create, receive, maintain, or transmit PHI on Business Associate’s behalf, enter into a written contract that contains the same terms, restrictions, requirements, and conditions as the HIPAA compliance provisions in this Contract with respect to such PHI. The same provisions must also be included in any contracts by a Business Associate’s Subcontractor with its own business associates as required by 45 CFR 164.314(a)(2)(b) and 164.504(e)(5).
    2. Obligations. To the extent the Business Associate is to carry out one or more of HCA’s obligation(s) under Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information), Business Associate must comply with all requirements that would apply to HCA in the performance of such obligation(s).
    3. Liability. Within ten (10) business days, Business Associate must notify the contact identified in Subsection 9.2 of any complaint, enforcement or compliance action initiated by the Office for Civil Rights based on an allegation of violation of the HIPAA Rules and must inform HCA of the outcome of that action. Business Associate bears all responsibility for any penalties, fines or sanctions imposed against the Business Associate for violations of the HIPAA Rules and for any imposed against its Subcontractors or agents for which it is found liable.
    4. Breach Notification.
       1. In the event of a Breach of unsecured PHI or disclosure that compromises the privacy or security of PHI obtained from HCA or involving HCA clients, Business Associate will take all measures required by state or federal law.
       2. Business Associate will notify the contact identified in Subsection 9.2 by telephone and in writing within five (5) business days of any acquisition, access, use or disclosure of PHI not allowed by the provisions of this DSA or not authorized by HIPAA Rules or required by law that potentially compromises the security or privacy of the Protected Health Information.
       3. Business Associate will notify the HCA Privacy Officer identified in Section 9.2 above by telephone or e-mail within five (5) business days of any potential Breach of security or privacy of PHI by the Business Associate or its Subcontractors or agents. Business Associate will follow telephone or e-mail notification with a written (fax or email acceptable) explanation of the Breach, to include the following: date and time of the Breach, date Breach was discovered, location and nature of the PHI, type of Breach, origination and destination of PHI, Business Associate unit and personnel associated with the Breach, detailed description of the Breach, anticipated mitigation steps, and the name, address, telephone number, fax number, and e-mail of the individual who is responsible as the primary point of contact. Business Associate will notify HCA prior to dissemination of any public announcement of a data security Breach involving HCA’s data and include in any such required notifications, the planned date for the public announcement.
       4. Solely for purposes of the performance of the Proof of Concept as more particularly set forth in Schedule 1 hereto and Schedules A hereto, if a Breach of unsecured PHI is the sole fault of Business Associate then as between Business Associate and HCA, Business Associate will remain liable for claims that may arise from such Breach, including, but not limited to, costs for litigation (including reasonable attorneys’ fees), and reimbursement sought by individuals, including but not limited to, costs for credit monitoring or allegations of loss in connection with the Breach, and to the extent that any claims are brought against HCA, must indemnify HCA from such claims (if such claims arise through no fault or breach by HCA) and Business Associate will be responsible for any other legal or regulatory obligations which may arise under applicable law in connection with such a Breach and will bear all costs associated with complying with legal and regulatory obligations in connection therewith. For avoidance of doubt, “fault” refers to the party’s failure through act or omission to use reasonable procedures to avoid unauthorized access, use or disclosure of Personal Information.
       5. In the event the Breach is the sole fault of HCA, then as between Business Associate and HCA, HCA will remain liable for claims that may arise from such Breach, including, but not limited to, costs for litigation (including reasonable attorneys’ fees), and reimbursement sought by individuals, including but not limited to, costs for credit monitoring or allegations of loss in connection with the Breach, and to the extent that any claims are brought against Business Associate, will indemnify Business Associate from such claims (if such claims arise through no fault or breach by Business Associate) and HCA will be responsible for any other legal or regulatory obligations which may arise under applicable law in connection with such a Breach and will bear all costs associated with complying with legal and regulatory obligations in connection therewith. For avoidance of doubt, “fault” refers to the party’s failure, through act or omission, to use reasonable procedures to prevent unauthorized acquisition of, access to or use of such Personal Information.
    5. Miscellaneous Provisions.
       1. Regulatory References. A reference in this DSA to a section in the HIPAA Rules means the section as in effect or amended.
       2. Interpretation. Any ambiguity in this DSA will be interpreted to permit compliance with the HIPAA Rules.
14. Inspection

HCA reserves the right to monitor, audit, or investigate compliance with this Contract in regards to the Personal Information and PHI of Enrollees collected, used, or acquired by Contractor during the term of this Contract and for six (6) years following termination or expiration of this Contract. HCA will have access to Contractor’s records and place of business for this purpose. All HCA representatives conducting onsite audits of Contractor agree to keep confidential any patient-identifiable information which may be reviewed during the course of any site visit or audit.

1. Indemnification for Unauthorized Use or Release

The Contractor must indemnify and hold HCA and its employees harmless from any damages related to the Contractor’s or Subcontractor’s unauthorized use or release of Personal Information or PHI of Enrollees.

|  |  |  |
| --- | --- | --- |
| User Agreement on Non-Disclosure of Confidential Information | | |
| Your organization has entered into a Contract with the state of Washington Health Care Authority (HCA) that will allow you access to data and records that are deemed Confidential Information as defined below. Prior to accessing this Confidential Information you must sign this *User Agreement on Non-Disclosure of Confidential Information.* | | |
| Confidential Information | | |
| “Confidential Information” means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information includes, but is not limited to, Protected Health Information and Personal Information. For purposes of the pertinent Contract, Confidential Information means the same as “Data.”  “Protected Health Information” means information that relates to: the provision of health care to an individual; the past, present, or future physical or mental health or condition of an individual; or the past, present or future payment for provision of health care to an individual and includes demographic information that identifies the individual or can be used to identify the individual.  “Personal Information” means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver license numbers, credit card numbers, any other identifying numbers, and any financial identifiers. | | |
| Regulatory Requirements and Penalties | | |
| State laws (including, but not limited to, RCW 74.04.060, RCW 74.34.095, and RCW 70.02.020) and federal regulations (including, but not limited to, HIPAA Privacy and Security Rules, 45 CFR Part 160 and Part 164; Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR, Part 2; and Safeguarding Information on Applicants and Beneficiaries, 42 CFR Part 431, Subpart F) prohibit unauthorized access, use, or disclosure of Confidential Information. Violation of these laws may result in criminal or civil penalties or fines. | | |
| User Assurance of Confidentiality | | |
| In consideration for HCA granting me access to the Confidential Information that is the subject of this Agreement, I agree that I:   1. Will access, use, and disclose Confidential Information only in accordance with the terms of this Agreement and consistent with applicable statutes, regulations, and policies. 2. Have an authorized business requirement to access and use the Confidential Information. 3. Will not use or disclose any Confidential Information gained by reason of this Agreement for any commercial or personal purpose, or any other purpose that is not directly connected with this Agreement. 4. Will not use my access to look up or view information about family members, friends, the relatives or friends of other employees, or any persons who are not directly related to my assigned job duties. 5. Will not discuss Confidential Information in public spaces in a manner in which unauthorized individuals could overhear and will not discuss Confidential Information with unauthorized individuals, including spouses, domestic partners, family members, or friends. 6. Will protect all Confidential Information against unauthorized use, access, disclosure, or loss by employing reasonable security measures, including physically securing any computers, documents, or other media containing Confidential Information and viewing Confidential Information only on secure workstations in non-public areas. 7. Will not make copies of Confidential Information, or print system screens unless necessary to perform my assigned job duties and will not transfer any Confidential Information to a portable electronic device or medium, or remove Confidential Information on a portable device or medium from facility premises, unless the information is encrypted and I have obtained prior permission from my supervisor. 8. Will access, use or disclose only the “minimum necessary” Confidential Information required to perform my assigned job duties. 9. Will not distribute, transfer, or otherwise share any software with anyone. 10. Will forward any requests that I may receive to disclose Confidential Information to my supervisor for resolution and will immediately inform my supervisor of any actual or potential security breaches involving Confidential Information, or of any access to or use of Confidential Information by unauthorized users. 11. Understand at any time, HCA may audit, investigate, monitor, access, and disclose information about my use of the Confidential Information and that my intentional or unintentional violation of the terms of this Agreement may result in revocation of privileges to access the Confidential Information, disciplinary actions against me, or possible civil or criminal penalties or fines. 12. Understand that my assurance of confidentiality and these requirements will continue and do not cease at the time I terminate my relationship with my employer. | | |
| Signature | | |
| Print User’s Name | User Signature | Date |
|  |  |  |